TLDR

Background

WPAD is short for Web Proxy Autodiscovery Protocol, and it is a protocol used by web browsers to discover the Proxy Auto Config (PAC) file. Web Browser traffic is usually directed through a proxy in many corporate environments. This might be done in order to terminate TLS, to be able to log or filter the workers web traffic. But when a computer is connected to a network, how does the webbrowser know where the proxy is?

WPAD is supported by most Web Browsers and OS, but is only endabled by default on Windows and Explorer/Edge.

Where the proxy can be found is defined in a file called PAC (Proxy Auto Config).

The browser discovers the PAC file in the following order:

1. It received the addrss to the PAC-file from the DHCP server.
2. I asks the local DNS server, in this order:

A computer with the following network name computer.team.division.company.example would look in the following locations, in order:

wpad.team.division.company.example/wpad.dat wpad.division.company.example/wpad.dat wpad.company.example/wpad.dat

3. It uses LLMNR/NBT-NS to ask for the wpad-subdomain.

PAC delivered over DHCP

If a machine performs a DHCP request with the code 252, the DHCP server till respond with the URL to the PAC file. For example: http://server.domain/proxyconfig.pac. The client then proceeds to request this JavaScript file, and the browser executes the file. When the JavaScript inside the PAC file is executed the Browser is instructed to use the, from the PAC defined, proxy server.

The obvious attack then becomes to set up a rouge DHCP server that responds with a malicious PAC file that instruct the web browser to send traffic the attackers proxy.

NBT-NS

If the local DNS server cannot resolve wpad.example.local the computer will use the NBT-NS protocol to try to resolve it. And any computer on the network can respond to the NBT-NS DNS request. So the malicious user can simply respond and say that the wpad.example.local can be found at the attackers IP-address.

How to exploit

Why is it not working?

On windows 10 and Windows Server 2008 R2 and later, https://www.alexandreviot.net/2015/01/03/dns-remove-wpad-filtering/

How to test for

In order to check

Recommendation

Create a DNS entry for wpad.

If no web proxy is used it is possible to disable the default usage of "Autodetect Proxy Settings".

References